Custer Telephone Cooperative Inc.

PO Box 324 • 1101 E. Main Ave. Challis, ID. 83226 • Telephone: (208) 879 2281 • Fax: (208) 879 5211

February 25, 2011

VIA ELECTRONIC FILING
Marlene H. Dortch, Secretary
Federal Communications Commission
445 12th Street, SW
Washington, DC 20554

RE: EB Docket 06-36
Custer Telephone Cooperative, Inc.
499 Filer ID: 806388
Annual CPNI Compliance Certification for Calendar Year 2010

Dear Ms. Dortch:

Pursuant to 47 C.F.R. § 64.2009(e), the undersigned, an officer of Custer Telephone Cooperative, Inc. (hereinafter referred to as the "Company") certifies based on personal knowledge that the Company has established and implemented policies and procedures to ensure that it complies with the Commission's rules regarding customer proprietary network information ("CPNI") found in 47 C.F.R. Part 64, Subpart U, with respect to all services subject thereto.

The Company has developed a written CPNI Policy and has implemented procedures to ensure compliance with the Policy and the CPNI rules. These policies and procedures, which are briefly summarized below, ensure compliance by limiting access to, use of, and disclosure of CPNI.

Only authorized personnel may access CPNI. All personnel so authorized, such as customer service representatives and billing and collection personnel, are trained in the appropriate access to, use of, and disclosure of CPNI. Managerial personnel receive similar training. The Company utilizes an electronic system to track employee access to CPNI, and employees must report instances of unauthorized access to or disclosure of CPNI. Failure to abide by the applicable policies and procedures is cause for discipline, up to and including termination.

The Company discloses call detail information to customers only after verifying the identity of the customer. Except for business customers with dedicated account representatives and whose contracts require other verification methods, customers must verify their identity by presenting a government-issued identification or by providing a pre-established password. Customers who have forgotten their passwords can verify their identity by providing pre-established backup

information. Passwords and backups do not use readily-available biographical information. In the alternative, the Company may mail call detail information to the customer or call the customer at the served telephone number. Employees are required to report instances of suspected pretexting.

Additional safeguards, such as firewalls and intrusion prevention systems, are used to prevent and to detect efforts to gain unauthorized access to electronic systems containing CPNI.

Notices are sent to customers whenever a password, back-up, or address of record is changed. Notices also are sent whenever on-line account access is initiated. These notices do not include the new account information or reveal the changed information.

The Company does not share CPNI among its affiliates, unless prior customer approval has been obtained or no customer approval is needed. Further, the Company shares CPNI with independent contractors and joint venture partners only after obtaining opt-in approval from customers. It also requires independent contractors and joint venture partners that have access to CPNI to enter an appropriate confidentiality agreement and to abide by applicable laws, regulations, policies, and procedures. The Company does not disclose CPNI to other third parties except as directed by the customer or as required by law.

The Company notifies customers of their right to restrict access to, use of, and disclosure of their CPNI. Periodic notices and one-time notices are provided as appropriate. Such notices may be provided through multiple methods, such as bill inserts, bill messages, notices published in the telephone directory, notices included on the Company's website, and oral notice provided during a telephone contact. The Company maintains records of all notices and approvals for at least one year.

All out-bound marketing campaigns that utilize CPNI are subject to managerial approval and to verification of customer approval to use CPNI in this manner. Records related to such efforts are maintained for at least one year.

Managerial personnel monitor access to, use of, and disclosure of CPNI on an on-going basis to ensure compliance with the applicable policies and procedures and to evaluate their effectiveness. The Company will report to the Commission instances, if any, in which opt-out mechanisms do not work properly.
The Company will report security breaches via the Federal Communications Commission's website as soon as practicable but no later than seven days after discovery. The Company will notify customers of each breach on or after the eighth day after reporting it unless law

enforcement directs otherwise. The Company maintains records of breaches for at least two years.

During the certification year, the Company neither has instituted proceedings nor has filed any petitions against data brokers; nor has the Company received information to suggest that pretexters have attempted to gain access to its customers' CPNI. The Company has received no customer complaints in the past year regarding unauthorized access to or disclosure of CPNI.

In addition, the Company has developed and implemented a written Identity Theft Prevention Policy ("ITPP") in compliance with regulations of the Federal Trade Commission. The ITPP incorporates and builds upon the CPNI Policy in order to provide additional protection for consumer information and to ensure consistency between the CPNI Policy and the ITPP.

Sincerely,

Dennis L. Thornock
General Manager